HEALTH AFFAIRS

TRICARE
Management
Activity

Steps to HIPAA Security Compliance

HIPAA Training: Summer Sessions

TMA Privacy Office

Agenda

- HIPAA Security Officers Training Completed: Now What?
  - Key Personnel
  - Compliance Assessment Preparation
  - Implementation

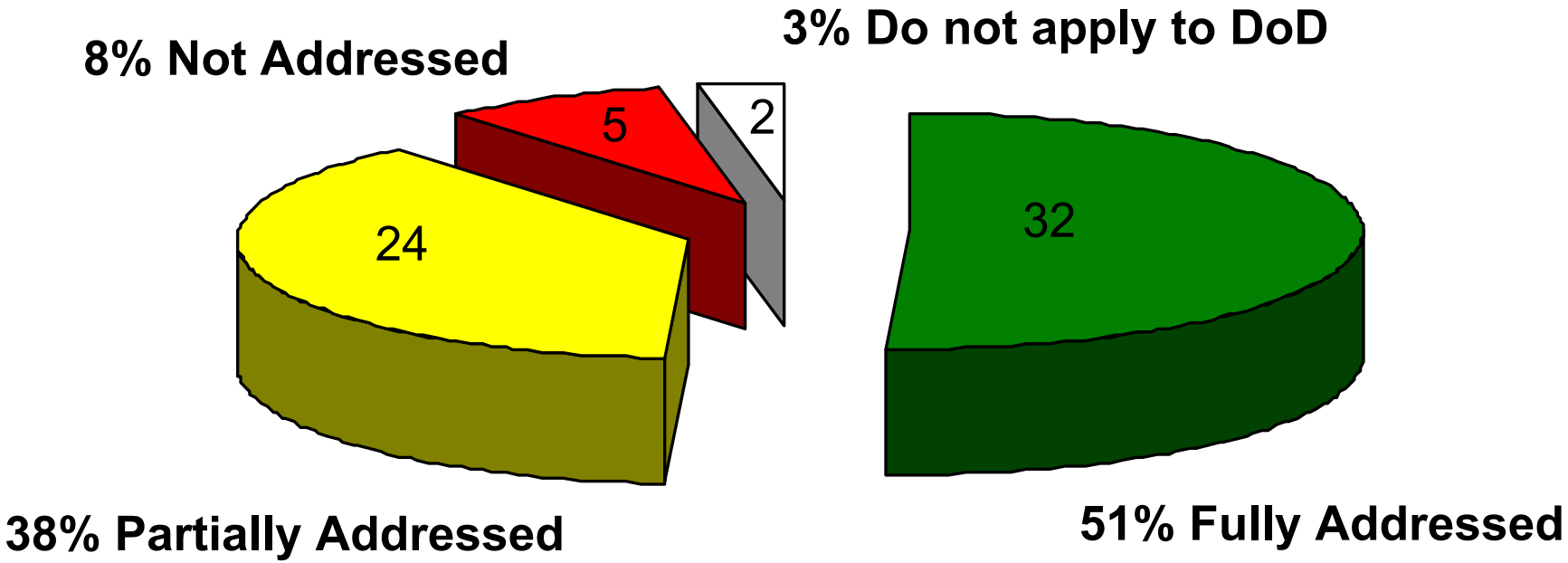
Training Objectives

- Upon completion of this course you should be able to:
  - Identify the steps required to reach HIPAA security compliance
  - Identify current activities and personnel that will assist you in meeting HIPAA security compliance
  - Identify the overlap between existing security program requirements and HIPAA Security implementation

HIPAA Implementation Life Cycle

New Requirements?

- Most HIPAA security standards and implementation specifications are fully addressed or partially addressed by DoD regulations



Compliance Assessment Activity

- Individually, complete the Compliance Assessment Matrix
  - Draw from your experience to identify activities that fall in each phase of an assessment
- You have 15 minutes to complete the matrix

Steps to HIPAA Security Compliance

- Key Personnel
  - First step: Appoint a HIPAA Security Officer in writing and identify other personnel within the organization that will support the implementation
- Compliance Assessment Preparation
- Implementation

Key Personnel

Key Personnel

Objectives

- Upon completion of this lesson, you should be able to:
  - Identify HIPAA security responsibility requirements
  - Identify key organizational personnel that will support HIPAA security implementation

Key Personnel

HIPAA Security Officer

- Assigned Security Responsibility*
  - A security officer must be appointed in writing to be responsible for the implementation of HIPAA security at each MTF
    - Store and maintain the appointment letter according to documentation requirements in the Security Rule
  - The security officer will serve as the focal point for security compliance related activities and responsibilities

*Ref: HIPAA Security Rule

Key Personnel: HIPAA Security Officer

Location of Draft Appointment Letters

- http://www.tricare.osd.mil/tmaprivacy/hipaa/hipaasecurity/securityofficers/index.htm

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (1 of 6)

- Manage the development and implementation of security policies, standards, guidelines, and procedures to ensure ongoing maintenance of the security of health information and compliance with the HIPAA Security Rule
- Monitor day-to-day entity operations and systems for compliance. Report to management on the status of compliance
- Periodically assess current security compliance status vs. necessary status (gap analysis)

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (2 of 6)

- Identify and review the security features of existing and new computing systems to ensure that they meet the security requirements of existing policies. Review and propose changes to existing policies and procedures that reflect the existing requirements of the systems to which they apply. Periodically reassesses status and updated security standards established by the facility

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (3 of 6)

- Work with management, the medical staff, the director of health information management, the privacy officer (if appointed separately), and others to ensure protection of patient privacy and confidentiality in a manner that does not compromise the entity, its personnel, good medical practice, or proper health information management practices
- Develop and/or ensure internal controls are capable of preventing and detecting significant instances or patterns of illegal, unethical, or improper conduct

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (4 of 6)

- Coordinate or oversee the filing of regulatory forms, reports, etc. Assist other departments in understanding and complying with regulatory requirements. Work with appropriate individuals to ensure facility implements and maintains appropriate security forms, materials, processes, procedures, and practices
- Coordinate and oversee regulatory submissions and reporting activities

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (5 of 6)

- Respond to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures
- Identify potential areas of compliance vulnerability and risk; develop/implement corrective action plans for the resolution of problematic issues and provide guidance on how to avoid or deal with similar situations

Key Personnel: HIPAA Security Officer

Policy Implementation, Oversight, Auditing and Compliance Duties (6 of 6)

- Establish and chair an institutional Compliance Committee to bring entity into overall compliance. Assure the committee consists of relevant personnel appropriate for the purpose
- Perform internal audit of data access and use to detect and deter breaches
- Receive reports of Security breaches, take appropriate action to minimize harm, investigate breaches, and make recommendations to management for corrective action

Key Personnel: HIPAA Security Officer

Education, Training, and Communication Responsibilities (1 of 3)

- Provide facility's information security policies and practices for employees and others with access to health information. Prepare and publish papers/articles on good security practices for facility's employees and others. Ensure that training conforms to existing policies and procedures
- Communicate the importance of compliance and the compliance program to senior management, the compliance committee, and other members of the healthcare workforce

Key Personnel: HIPAA Security Officer

Education, Training, and Communication Responsibilities (2 of 3)

- Education, Training, and Communication (Cont.)
  - Promote the use of the compliance help-line, increase awareness of integrity and compliance and foster understanding of new and existing compliance issues and related policies and procedures
  - Work with leadership to ensure that they and all employees have the requisite information and knowledge of regulatory issues and requirements to carry out their responsibilities in a lawful and ethical manner

Education, Training, and Communication Responsibilities (3 of 3)

- Education, Training, and Communication (Cont.)
  - Provide input and/or direction to the employee performance appraisal and incentive programs to ensure improper conduct is reported and discouraged and that support of and conformity with the compliance program is part of any performance evaluation process for all employees

Key Personnel: HIPAA Security Officer

MTF Integration Activities

- Work in cooperation with human resources, administration, and legal counsel, as appropriate to ensure consistent action is taken for failure to comply with security policies for all employees on the workforce
- Function as key representative/liaison in meetings regarding regulatory policy

Key Personnel

Medical Information Security Readiness Team (MISRT)

- All MTFs should appoint interdisciplinary teams that include clinical, administration, and information technology personnel
- The Surgeon's General of the Army, Navy and Air Force directed that MISRTs be formed by January 2001 in every MTF

Key Personnel

MISRT Responsibilities

- Coordination of HIPAA data security compliance program including policies, procedures and practices
- Supervision of information security risk assessment & risk management
- Coordination of training in health information assurance
- Coordination of development of technical security infrastructure
- Oversight of certification and accreditation of medical information systems

Other Personnel

- Other personnel that can provide assistance for the implementation of HIPAA security include:
  - Senior Executive Team POC
  - Medical Risk Management Team
  - Head of Administration Department
  - Physical Security Officer
  - Chief Information Officer
  - Joint Commission on Accreditation of Healthcare Organizations (JCAHO) Coordinator
  - Information Systems Security Manager
  - Information Systems Security Officer
  - FISMA Coordinator

Summary

- You should now be able to:
  - Identify HIPAA security responsibility requirements
  - Identify key organizational personnel that will support HIPAA security implementation

Steps to HIPAA Security Compliance

- Key Personnel
  - First step: Appoint a HIPAA Security Officer in writing and identify other personnel within the organization that will support the implementation
- Compliance Assessment Preparation
  - Second step: Collect information required to complete the Compliance Assessment
- Implementation

Compliance Assessment Preparation

Objectives

- Upon completion of this lesson, you will be able to:
  - Identify the items that should be collected prior to starting the compliance assessment

Compliance Assessment Preparation

Information Systems

- Identify Information Systems
  - Determine the information systems that are utilized at the MTF
  - Identify which information systems process Electronic Protected Health Information (EPHI)
  - Identify a Point Of Contact (POC) (i.e., system owner, information systems security officer, etc.) for each information system

** Remember to include all Biomedical Devices

Compliance Assessment Preparation

Documentation (1 of 4)

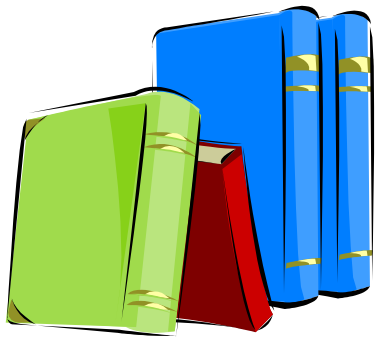
- Identify and Collect Required Documentation
  - **Security Management Process**: Policies and procedures that address the prevention, detection, containment, and correction of security violations
  - **Workforce Security**: Policies and procedures that address workforce access to data
  - **Information Access Management**: Policies and procedures that authorize access to data
  - **Security Awareness and Training**: Security Awareness and Training plan or applicable policies and procedures

Documentation (2 of 4)

- Identify and Collect Required Documentation (Cont.)
  - **Security Incident Procedures**: Computer Incident Response Plan or applicable policies and procedures
  - **Contingency Plan**: Contingency Plan, Data Backup Plan, Emergency Mode Operation Plan, or applicable policies and procedures
  - **Business Associate Contracts and Other Arrangements**: Contracts, Memorandums of Understanding, or Memorandums of Agreement

Documentation (3 of 4)

- Identify and Collect Required Documentation (Cont.)
  - **Facility Access Controls**: Facility Security Plan or applicable policies and procedures addressing physical access to information systems
  - **Device and Media Control**: Policies and procedures addressing the receipt and removal of hardware and media



Documentation (4 of 4)

- Identify and Collect Required Documentation (Cont.)
  - **Access Control**: Technical policies and procedures addressing access controls for information systems
  - **Integrity**: Policies and procedures addressing the protection of data from improper alteration or destruction

Summary

- You should now be able to:
  - Identify the items that should be collected prior to starting the compliance assessment

Activity

- Review the matrix and add any additional items to the Pre-Assessment Phase
- Work within large groups to complete this exercise
- You have 10 minutes

Steps to HIPAA Security Compliance

- Key Personnel
  - First step: Appoint a HIPAA Security Officer in writing and identify other personnel within the organization that will support the implementation
- Compliance Assessment Preparation
  - Second step: Collect information required to complete the Compliance Assessment
- Implementation
  - Third step: Implement the security requirements

Implementation

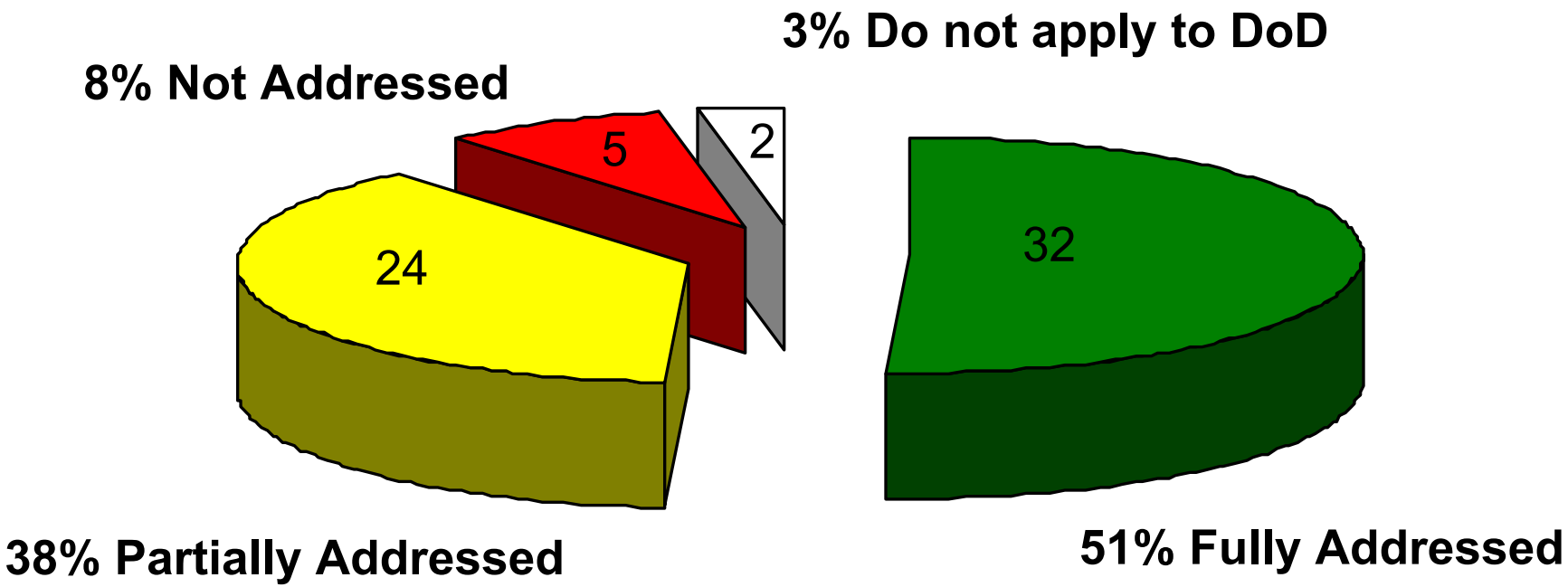
Implementation

Objectives

- Upon completion of this lesson, you should be able to:
  - Identify required steps to comply with each HIPAA security standard
  - Identify current activities that support compliance
  - Identify personnel within your facility that will assist in reaching compliance

New Requirements?

- Most HIPAA security standards and implementation specifications are fully addressed or partially addressed by DoD regulations



Requirements Not Addressed

- 5 requirements are not addressed
  - Not specifically addressed by DoD regulations
- Administrative Safeguards
  - Security Reminders
  - Protection from Malicious Software
  - Log-in Monitoring
  - Password Management
- Policies and Procedures and Documentation
  - Time Limit

Requirements Partially Addressed (1 of 5)

- 24 requirements are partially addressed
  - DoD level regulations apply to a wide range of environments
  - The details for security requirements are left to the Service or organization for determination and implementation
  - The intent is present, but not specifically documented
  - Documentation

Implementation

Requirements Partially Addressed (2 of 5)

- Administrative Safeguards
  - Workforce Clearance Procedures
  - Emergency Mode Operation Plan
  - Testing and Revision Procedure
  - Business Associate Contracts and Other Arrangements
  - Written Contract or Other Arrangements

Requirements Partially Addressed (3 of 5)

- Physical Safeguards
  - Access Control/Validation Procedures
  - Maintenance Records
  - Workstation Use
  - Device and Media Controls
  - Disposal
  - Media Re-use
  - Accountability
  - Data Backup and Storage

Requirements Partially Addressed (4 of 5)

- Technical Safeguards
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption
  - Encryption

Requirements Partially Addressed (5 of 5)

- Organizational Requirements
  - Business Associate Contracts or Other Arrangements
  - Business Associate Contracts (written)
  - Other Arrangements
- Policies and Procedures and Documentation
  - Policies and Procedures
  - Documentation

Implementation

HIPAA Security Standards

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Policies and Procedures and Documentation

Implementation

Administrative Safeguards

- Security Management Process
- Workforce Security
- Information Access Management
- Security Awareness & Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

Implementation: Administrative Safeguards

Security Management Process (1 of 5)

- Security Management Process
  - Implement policies and procedures to prevent, detect, contain, and correct security violations
- Fully addressed by DoD regulations

Implementation: Administrative Safeguards

Security Management Process (2 of 5)

- **Remember to** perform risk assessments for each individual information system
- Risk assessments typically include the following steps:
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation

Implementation: Administrative Safeguards

Security Management Process (3 of 5)

- Document the decisions concerning the administrative, physical, and technical controls selected to mitigate identified risks
  - Create local policies that clearly establish roles and responsibilities and assign ultimate responsibility for the implementation of each control to particular individuals or offices
  - Create procedures that support policies and to accomplish particular security related tasks

Implementation: Administrative Safeguards

Security Management Process (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - Physical Security Reviews
    - Head of Administration Department
  - FISMA Reporting
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Administrative Safeguards

Security Management Process (5 of 5)

- Sources

- DoD 5000.1-D, Defense Acquisitions
- DoD 5000.2-R, Mandatory Procedures for MDAS & MAIS Acquisition Programs
- DoD 5160.54-D, Critical Asset Assurance Program
- DoD 5200.40-I, Defense Information Technology Security Certification & Accreditation Process
- DoD 8000.1-D, Defense Information Management Program
- DoD 8500.1-D, Information Assurance
- DoD 8500.2-I, Information Assurance Implementation
- DoD 8510.1-M, DITSCAP Manual

DoD

- Ref §3544(a)(b)(1) "Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency."

FISMA

- IM.2: Confidentiality, security, and integrity of data and information are maintained

JCAHO

HIPAA

Implementation: Administrative Safeguards

Workforce Security (1 of 6)

- Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI
- One Implementation Specification is partially addressed by DoD regulations
  - Workforce Clearance Procedure

Implementation: Administrative Safeguards

Workforce Security (2 of 6)

- **Remember to** define roles and responsibilities for all job functions
- Assign appropriate levels of security oversight, training, and access
- Identify in writing who has the business need—*and who has been granted permission*—to view, alter, retrieve, and store electronic health information, and at what times, under what circumstances, and for what purposes

Implementation: Administrative Safeguards

Workforce Security (3 of 6)

- Ensure that staff members have the necessary knowledge, skills, and abilities to fulfill particular roles
- Ensure that the workforce security requirements are included as part of the personnel hiring process
- Develop a standard set of procedures that should be followed to terminate access when employment or assignment ends
  - Recover access control devices (Identification [ID] badges, keys, access cards, etc.)
  - Deactivate computer access accounts
  - Disable user IDs and passwords

Implementation: Administrative Safeguards

Workforce Security (4 of 6)

- **In addition**, analyze positions to determine background check requirements (e.g., positions involving access to and use of sensitive information (PHI))
  - Implement as necessary

Implementation: Administrative Safeguards

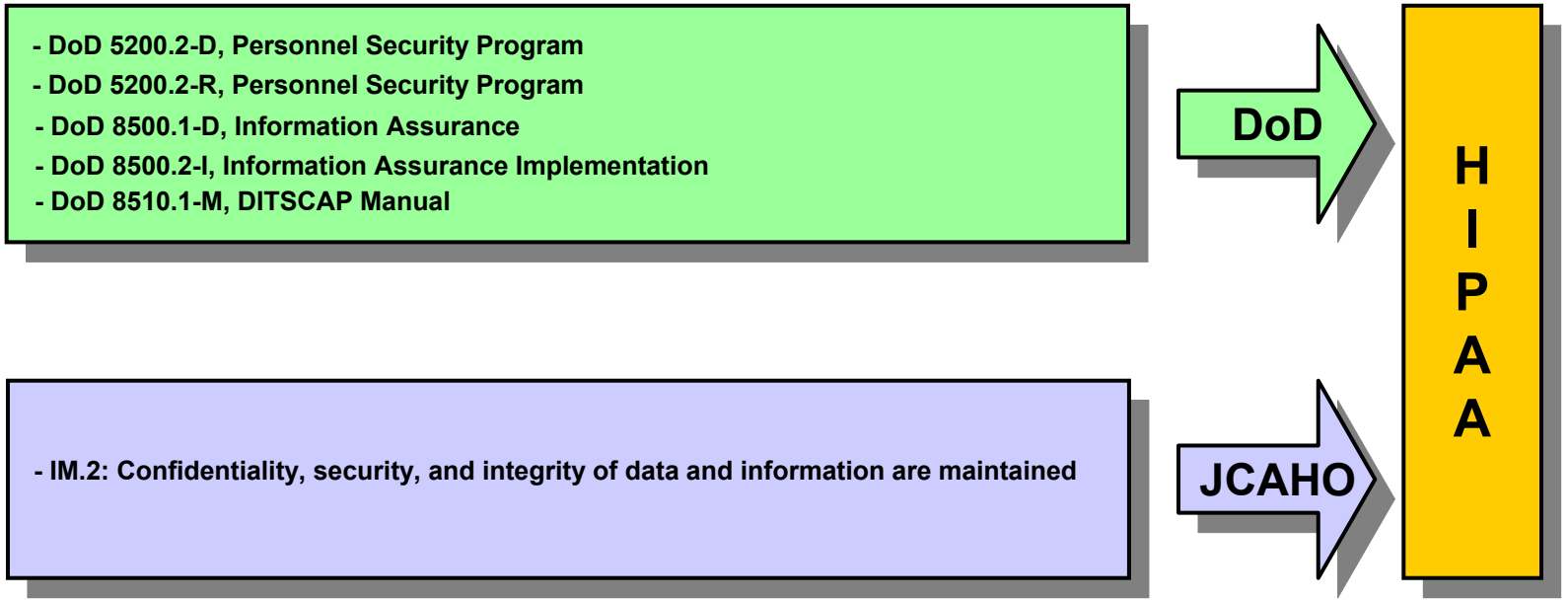
Workforce Security (5 of 6)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - Personnel Reviews
    - Head of Administration Department
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Administrative Safeguards

Workforce Security (6 of 6)

- Sources



Information Access Management (1 of 5)

- Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule
- Fully addressed by DoD regulations

Implementation: Administrative Safeguards

Information Access Management (2 of 5)

- **Remember to** coordinate with business process owners
- Establish standards for granting access
  - Choose between identity-based access (by name) or role-based access (by position or by other appropriate means)
  - Determine which positions require access to what information
  - Align these access policies with the Privacy Rule
- Document the process used to grant access

Implementation: Administrative Safeguards

Information Access Management (3 of 5)

- Provide formal authorization from the appropriate authority before granting access to sensitive information
- Decide and document how the person with the assigned security responsibility will consistently grant access to others within the organization
- Evaluate access controls already in place or implement new access controls as appropriate
- Align with other existing administrative, physical, and technical safeguards

Implementation: Administrative Safeguards

Information Access Management (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - Personnel Reviews
    - Head of Administration Department
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Administrative Safeguards

Information Access Management (5 of 5)

- Sources

- DoD 8500.1-D, Information Assurance
- DoD 8500.2-I, Information Assurance Implementation
- DoD 8510.1-M, DITSCAP Manual

DoD

Ref §3544(b)(2) "policies and procedures that-(A) are based on the risk assessments required by paragraph (1);(B) cost-effectively reduce information security risks to an acceptable level; (C) ensure that information security is addressed throughout the life cycle of each agency information system; and (D) ensure compliance with-(i) the requirements of this subchapter; (ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40; (iii) minimally acceptable system configuration requirements, as determined by the agency; and (iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President...."

FISMA

- IM.2: Confidentiality, security, and integrity of data and information are maintained
- IM.1 The hospital plans and designs information management processes to meet internal and external information needs.

JCAHO

HIPAA

Implementation: Administrative Safeguards

Security Awareness & Training (1 of 9)

- Implement a security awareness and training program for all members of its workforce (including management)
- Four Implementation Specifications are not addressed by DoD regulations:
  - Security Reminders
  - Protection from Malicious Software
  - Log-in Monitoring
  - Password Management

Security Awareness & Training (2 of 9)

- **Remember to** determine the HIPAA training needs of the organization
  - Interview and involve key personnel in assessing security training needs
- Evaluate the awareness and training program in place
- Address the specific HIPAA policies that require awareness and training in your organization's written training strategy

Implementation: Administrative Safeguards

Security Awareness & Training (3 of 9)

- Outline in the written training plan
  - Scope of the awareness and training program
  - Goals
  - Target audiences
  - Learning objectives
  - Deployment methods, evaluation, and measurement techniques
  - Frequency of training

Implementation: Administrative Safeguards

Security Awareness & Training (4 of 9)

- Deliver training information to staff in the most effective and cost-efficient manner
- Consider using a variety of media and avenues according to what is appropriate for the organization based on workforce size, location, level of education, etc
- Schedule and conduct the training outlined in the strategy and plan

Implementation: Administrative Safeguards

Security Awareness & Training (5 of 9)

- Implement any reasonable technique to disseminate the security messages in an organization, including newsletters, screensavers, videotapes, e-mail messages, teleconferencing sessions, staff meetings, and computer-based training
- Keep the security awareness and training program relevant and timely

Implementation: Administrative Safeguards

Security Awareness & Training (6 of 9)

- Conduct training whenever changes occur in the technology and practices as appropriate
- Monitor and track the training program implementation to ensure all employees participate
  - Document as required (e.g., attendance and training costs)
- Implement corrective actions when issues arise
- **In addition**, ensure that security reminders are issued to employees on are periodic basis

Security Awareness & Training (7 of 9)

- **In addition**, select the topics that may need to be covered in the training materials including the following:
  - Incident reporting
  - How to protect and guard the system from malicious software
  - Procedures for detecting and reporting malicious software
  - Procedures for monitoring log-in attempts and reporting discrepancies
  - Password management and use

Implementation: Administrative Safeguards

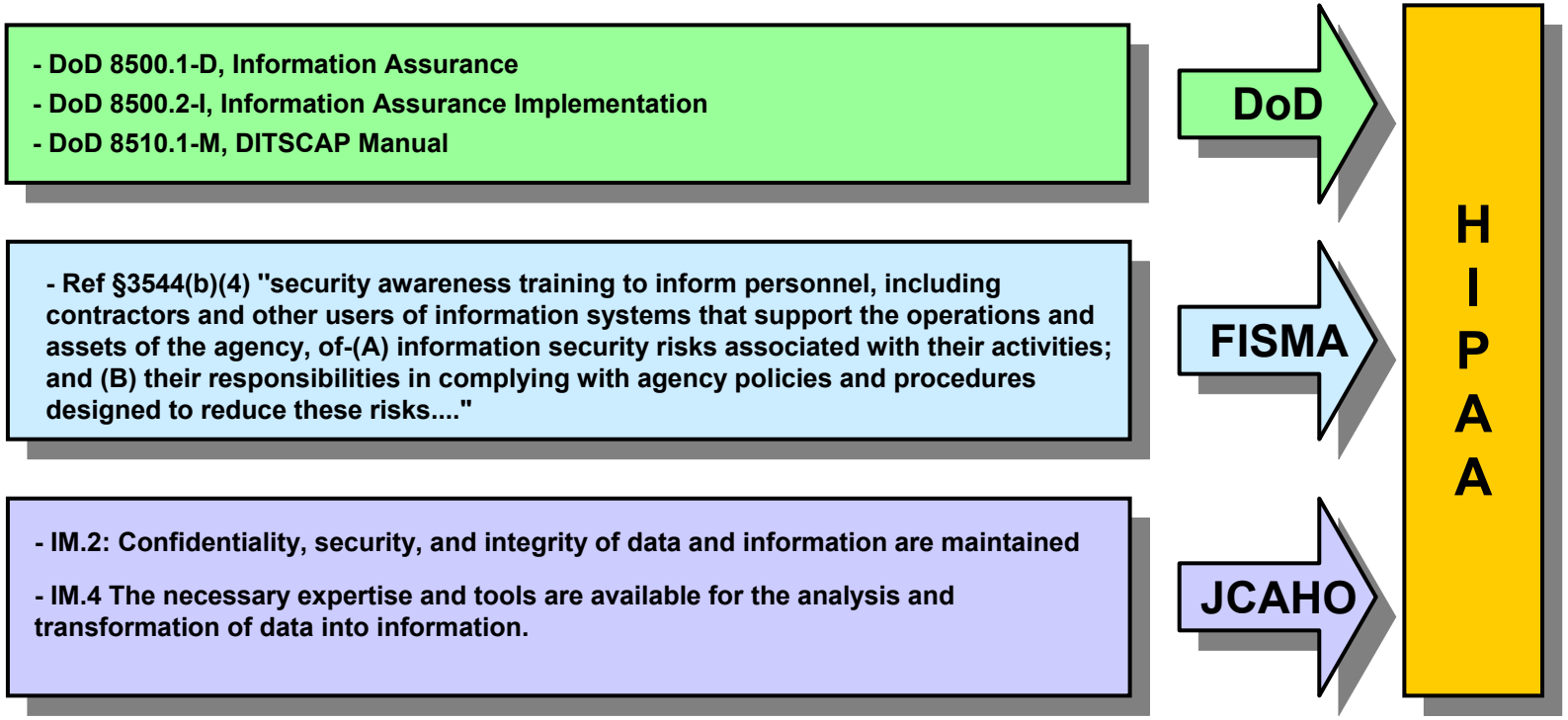
Security Awareness & Training (8 of 9)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator

Implementation: Administrative Safeguards

Security Awareness & Training (9 of 9)

- Sources



Security Incident Procedures (1 of 6)

- Implement policies and procedures to address security incidents
- Fully addressed by DoD regulations

Implementation: Administrative Safeguards

Security Incident Procedures (2 of 6)

- **Remember to** gain an understanding of existing security incident response procedures
- Determine how the organization will respond to a HIPAA security breach (i.e., notify the Privacy Officer if breach results in an unauthorized disclosure of PHI)
- Establish a reporting mechanism and a process to coordinate responses to the security incident

Security Incident Procedures (3 of 6)

- Provide direct technical assistance, advise vendors to address product-related problems, and provide liaisons to legal and criminal investigative groups as needed
- Identify appropriate individuals to be a part of a formal incident response team, when required
- Update documented incident response procedures
  - to include procedures for personnel that discover security violations
  - procedures to mitigate security incidents

Implementation: Administrative Safeguards

Security Incident Procedures (4 of 6)

- Document incident response procedures to provide a single point of reference to guide the day-to-day operations of the incident response team
- Review incident response procedures, solicit input, and make changes to reflect input
- Update the procedures as required based on changing organizational needs
- Measure effectiveness and update security incident response procedures to reflect lessons learned, and make recommendations for improvements to security controls after a security incident

Implementation: Administrative Safeguards

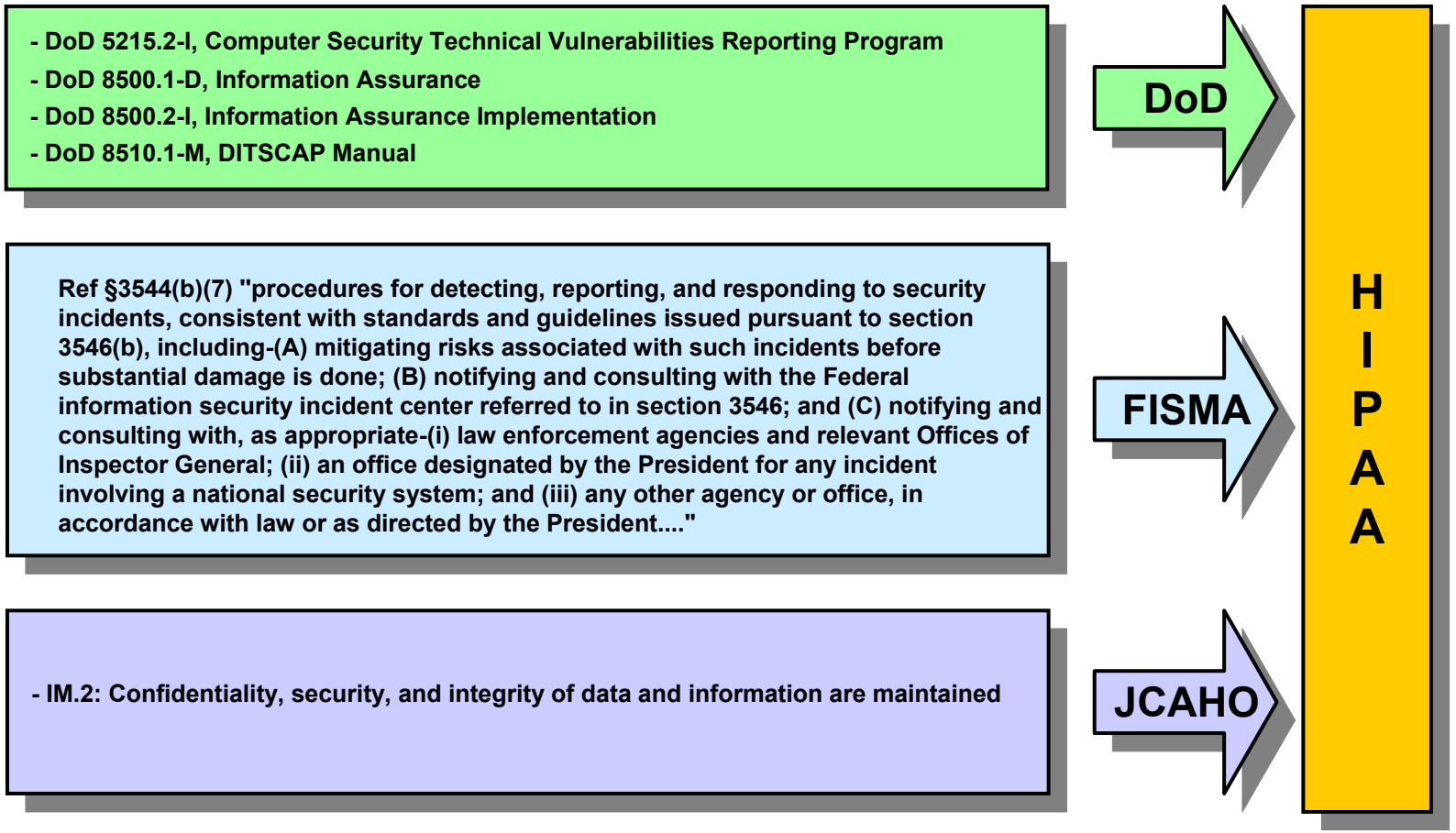
Security Incident Procedures (5 of 6)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Administrative Safeguards

Security Incident Procedures (6 of 6)

- Sources



Implementation: Administrative Safeguards

Contingency Plan (1 of 7)

- Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI
- Two Implementation Specifications are partially addressed by DoD regulations
  - Emergency Mode Operation Plan
  - Testing and Revision Procedure

Contingency Plan (2 of 7)

- **Remember that** contingency plans are not unique to HIPAA, rather contingency plans are a critical component to the business practices of your organization
- Contingency plans must:
  - Establish the organizational framework, roles, and responsibilities for contingency operations
  - Address scope, resource requirements, training, testing, plan maintenance, and backup requirements
  - Identify the critical services or operations and the manual and automated processes that support business operations

Implementation: Administrative Safeguards

Contingency Plan (3 of 7)

- Determine the amount of time the organization can tolerate power outages, disruption of services, and/or loss of capability
- Establish cost-effective strategies for recovering these critical services or processes
- Identify preventive measures for each defined scenario that could result in loss of a critical service operation
- Ensure identified preventive measures are practical and feasible in terms of their applicability in a given environment

Implementation: Administrative Safeguards

Contingency Plan (4 of 7)

- Finalize the set of contingency procedures that should be invoked for all identified impacts
- Ensure that formal agreements are in place when the strategy depends on external organizations for support
- Document all the decisions made in the previous steps
- Train those with defined plan responsibilities on their roles

Contingency Plan (5 of 7)

- **In addition**, ensure that it is documented how business will be done until full operations can be restored
- **In addition**, test the contingency plan on a predefined cycle and update documentation as required
  - If possible, involve external entities (vendors, alternative site/service providers) in testing exercises
  - Make key decisions regarding how the testing is to occur ("tabletop" exercise versus staging a real operational scenario including actual loss of capability)
  - Decide how to segment the type of testing based on the assessment of business impact and acceptability of sustained loss of service

Implementation: Administrative Safeguards

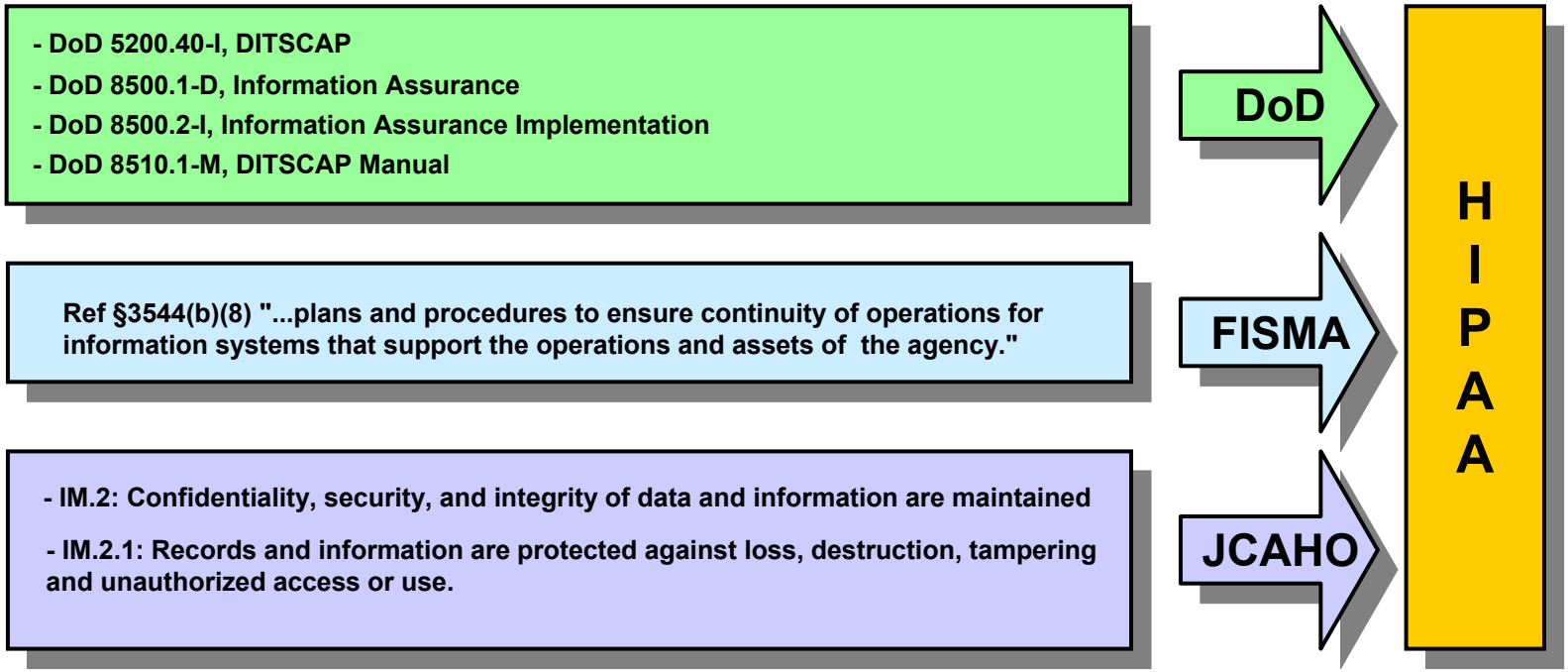
Contingency Plan (6 of 7)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - Physical Security Reviews
    - Head of Administration Department
  - IG Inspections
    - Chief Information Officer

Implementation: Administrative Safeguards

Contingency Plan (7 of 7)

- Sources



Implementation: Administrative Safeguards

Evaluation (1 of 8)

- Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under the Security Rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of the Security Rule
- Fully addressed by DoD regulations

Implementation: Administrative Safeguards

Evaluation (2 of 8)

- **Remember to** decide whether the evaluation will be conducted with internal staff resources or external consultants (engage external expertise to assist the internal evaluation team if additional skills and expertise is required)
  - External expertise can be internal to DoD or your service
- Use internal resources to supplement an external source of help, because these internal resources can provide the best institutional knowledge and history of internal policies and practices

Implementation: Administrative Safeguards

Evaluation (3 of 8)

- Use an evaluation strategy that has substance and can be tracked, including questionnaires and checklists, because documentation is key to demonstrating compliance
- Implement strategies that can provide reports on the level of compliance, integration, or maturity of a particular security safeguard
  - Leverage any existing reports or documentation that may already be prepared by the organization

Implementation: Administrative Safeguards

Evaluation (4 of 8)

- Secure management support for the evaluation process to ensure participation
- Determine, in advance, what departments and/or staff will participate in the evaluation
- Engage management, legal, or regulatory compliance staff when conducting the analysis
- Collect and document all needed information

Implementation: Administrative Safeguards

Evaluation (5 of 8)

- Analyze the evaluation results
- Identify security weaknesses
- Document in writing all findings and decisions

Implementation: Administrative Safeguards

Evaluation (6 of 8)

- Develop security program priorities and establish targets for continuous improvement
- Establish the frequency of evaluations, taking into account the sensitivity of the EPHI controlled by the organization, its size and complexity, and other relevant laws or accreditation requirements
- Repeat evaluations when significant changes to the security environment are made; for example, if new technology is adopted or if there are newly recognized risks to the security of the information

Implementation: Administrative Safeguards

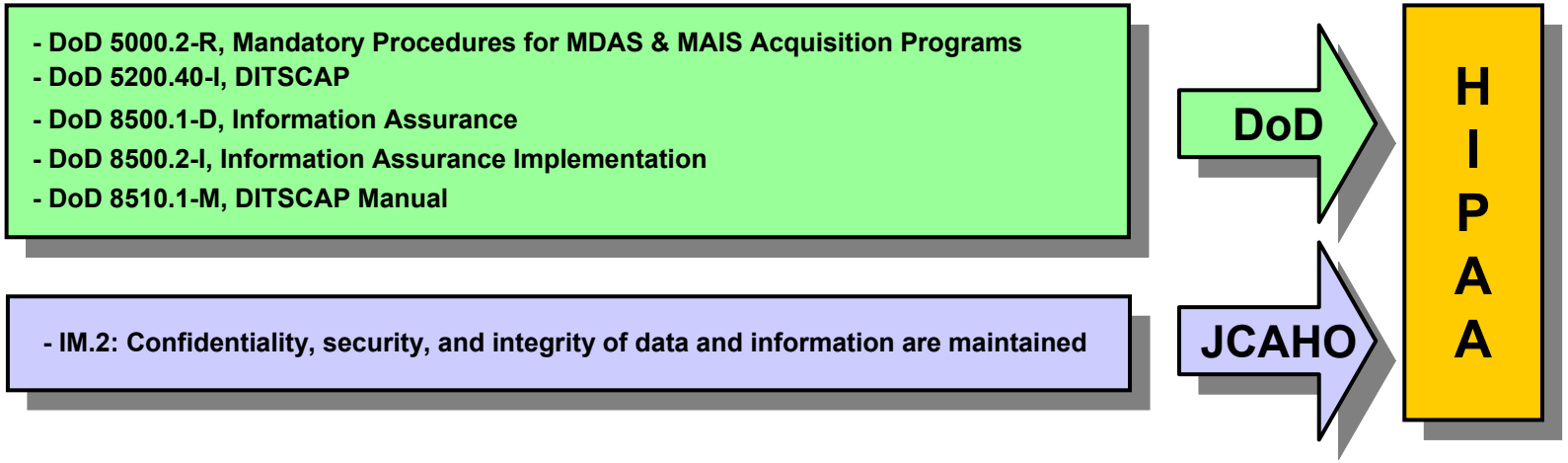
Evaluation (7 of 8)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - JCAHO Reviews
    - JCAHO Coordinator

Implementation: Administrative Safeguards

Evaluation (8 of 8)

- Sources



Business Associate Contracts and Other Arrangements (1 of 5)

- A covered entity may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate appropriately safeguards the information
- Standards and three Implementation Specifications are partially addressed by DoD regulations
  - Written Contract or Other Arrangements
  - Business Associate Contracts
  - Other Arrangements

Business Associate Contracts and Other Arrangements (2 of 5)

- **Remember to** identify the individual or department who will be responsible for coordinating the execution of business associate agreements
- Review the list of business associates to determine who has access to protected information to assess whether the list is complete and current
- Identify systems covered by the contract/agreement
- Identify roles and responsibilities

Business Associate Contracts and Other Arrangements (3 of 5)

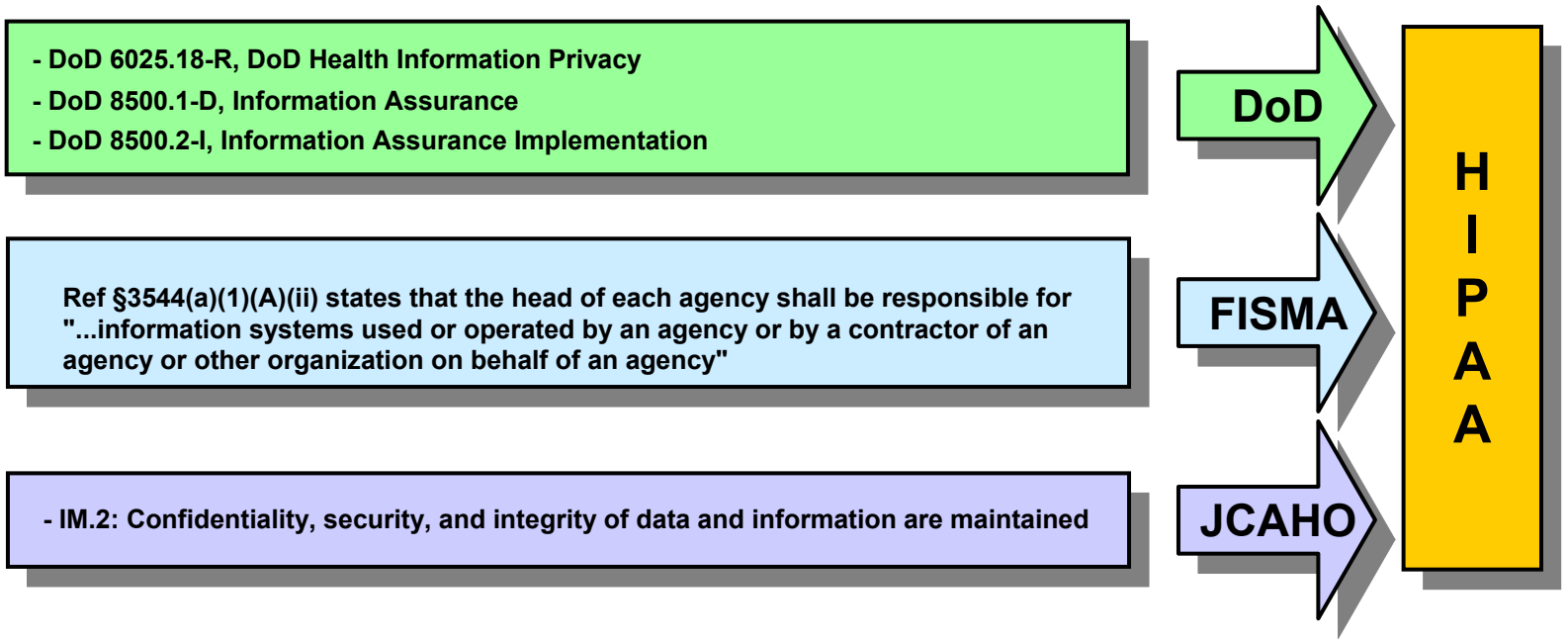
- Specify any training requirements associated with the contract/agreement
- Maintain clear lines of communication
- Conduct a review of security requirements specified in the contract
- Establish criteria for measuring contract performance (metrics)
- **In addition**, include security requirements in business associate contracts/agreements to address the security and privacy of PHI

Business Associate Contracts and Other Arrangements (4 of 5)

- Existing activities that support compliance:
  - HIPAA Privacy
    - HIPAA Privacy Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator

Business Associate Contracts and Other Arrangements (5 of 5)

- Sources



Implementation

Physical Safeguards

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Implementation: Physical Safeguards

Facility Access Controls (1 of 6)

- Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed
- Two Implementation Specifications are partially addressed by DoD regulations
  - Access Control/Validation Procedures
  - Maintenance Records

Facility Access Controls (2 of 6)

- **Remember to** inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities
  - Coordinate these activities with the facility's physical security officer
- Assign degrees of significance to each vulnerability identified
- Identify and assign responsibility for the measures and activities necessary to correct deficiencies

Facility Access Controls (3 of 6)

- Highest priority for remedial action should be on the following primary types of facilities:
  - Computer room
  - Peripheral equipment locations
  - IT staff offices
  - Workstation locations

Implementation: Physical Safeguards

Facility Access Controls (4 of 6)

- Document appropriate measures to provide physical security protection for EPHI in a covered entity's possession
- **In addition**, develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications made to the appropriate physical areas of the facility are documented
- **In addition**, develop policies and procedures to provide facility access to authorized personnel and visitors based on a need-to-know, including emergency response personnel

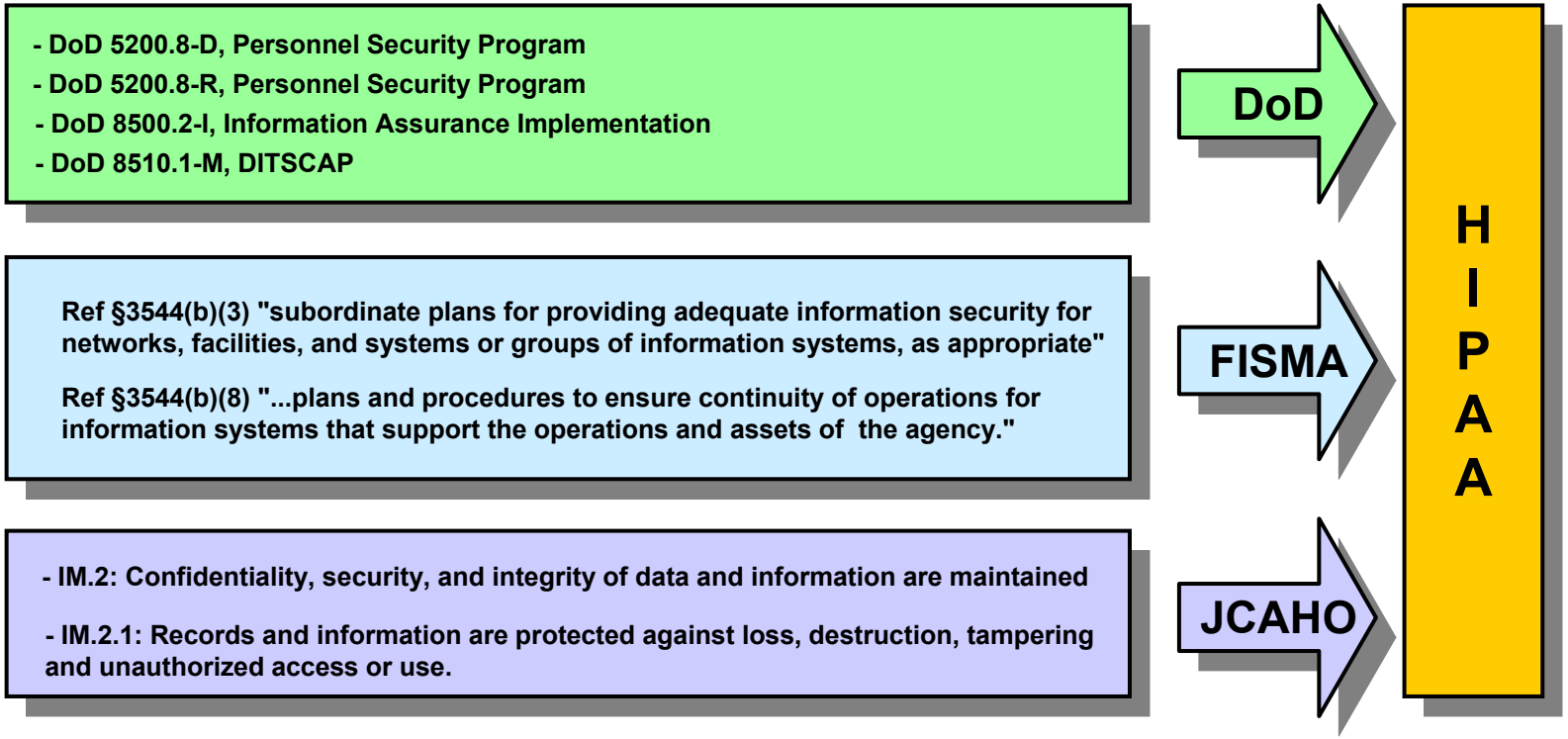
Facility Access Controls (5 of 6)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - Physical Security Reviews
    - Head of Administration Department
  - IG Inspections
    - Chief Information Officer

Implementation: Physical Safeguards

Facility Access Controls (6 of 6)

- Sources



Implementation: Physical Safeguards

Workstation Use (1 of 5)

- Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI
- Standard is partially addressed by DoD regulations

Implementation: Physical Safeguards

Workstation Use (2 of 5)

- **Remember to** inventory and categorize workstations and devices
- Develop policies and procedures for each type of workstation and workstation device based on their unique characteristics
- Develop and document policies and procedures related to the proper use and performance of workstations
- Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts

Implementation: Physical Safeguards

Workstation Use (3 of 5)

- Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations and limit the ability of unauthorized persons to view PHI
- **In addition**, categorize workstations based on the type of information, capabilities, connections, and allowable activities for each workstation used

Implementation: Physical Safeguards

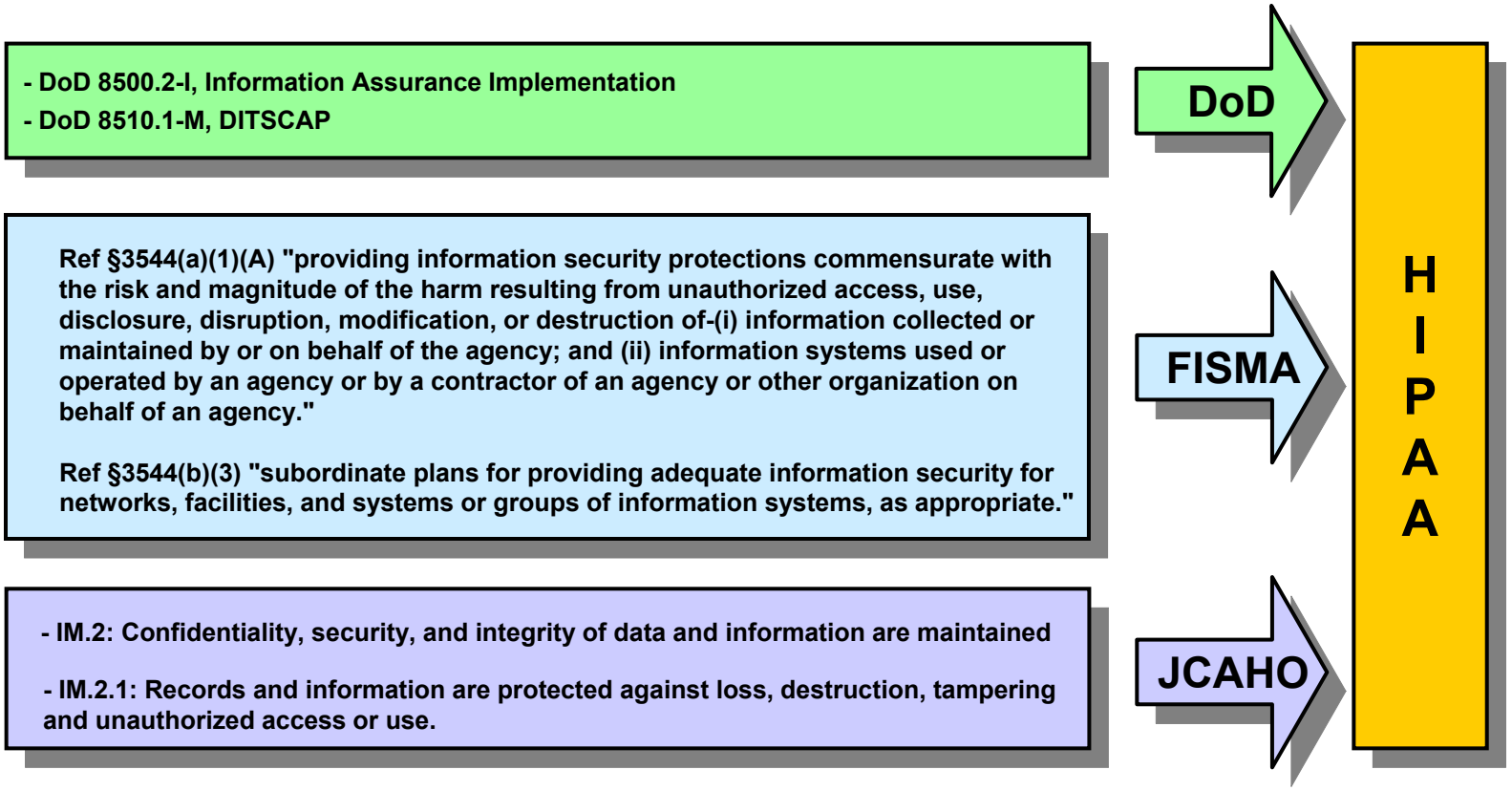
Workstation Use (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Physical Safeguards

Workstation Use (5 of 5)

- Sources



Implementation: Physical Safeguards

Workstation Security (1 of 4)

- Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users
- Fully addressed by DoD regulations

Implementation: Physical Safeguards

Workstation Security (2 of 4)

- **Remember to** document the different ways workstations can be accessed by employees and non-employees
- Determine the locations of workstations that access EPHI
- Determine which types of physical access create the greatest risk
- Document the options for deploying physical safeguards that will minimize the risk to security of EPHI and the equipment that processes EPHI

Implementation: Physical Safeguards

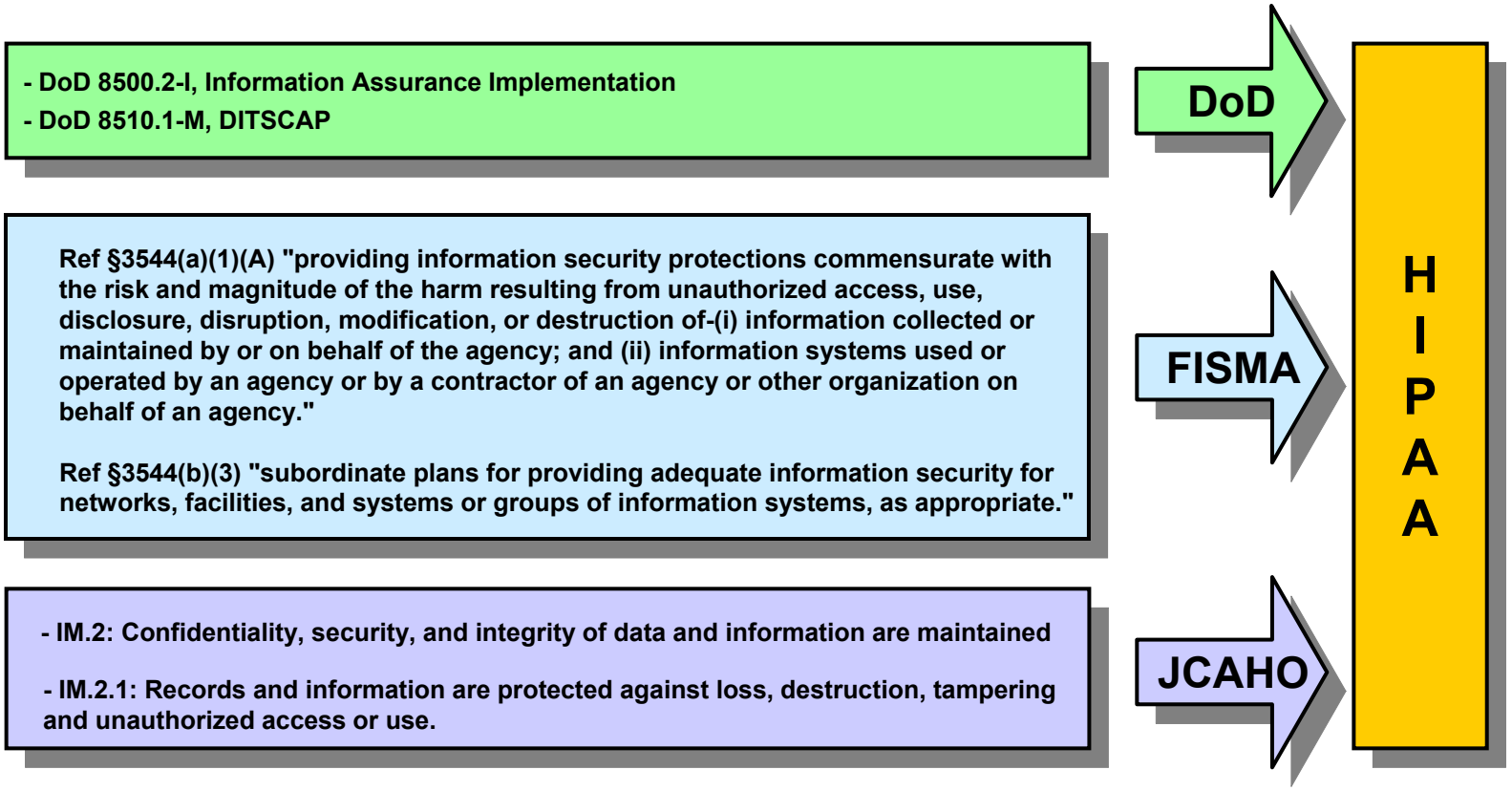
Workstation Security (3 of 4)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Physical Safeguards

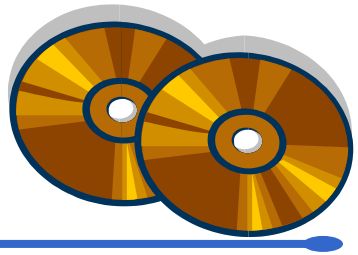
Workstation Security (4 of 4)

- Sources



Implementation: Physical Safeguards

Device and Media Controls (1 of 5)



- Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility
- Standard and four Implementation Specifications are partially addressed by DoD regulations
  - Disposal
  - Media Re-use
  - Accountability
  - Data Backup and Storage

Implementation: Physical Safeguards

Device and Media Controls (2 of 5)

- **Remember to** determine and document the appropriate methods to dispose of hardware, software, and the data itself
- Identify removable devices and their use
- Ensure that EPHI is properly destroyed and cannot be recreated when no longer needed
- Ensure that EPHI is not inadvertently released or shared with any unauthorized personnel

Device and Media Controls (3 of 5)

- Ensure that EPHI is not inadvertently transmitted to other systems
- **In addition**, ensure that EPHI previously stored on electronic media cannot be accessed when reused by any other user
- **In addition**, ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with EPHI at all times, and
- **In addition**, ensure that an exact, retrievable copy of the data is retained and protected prior to moving equipment

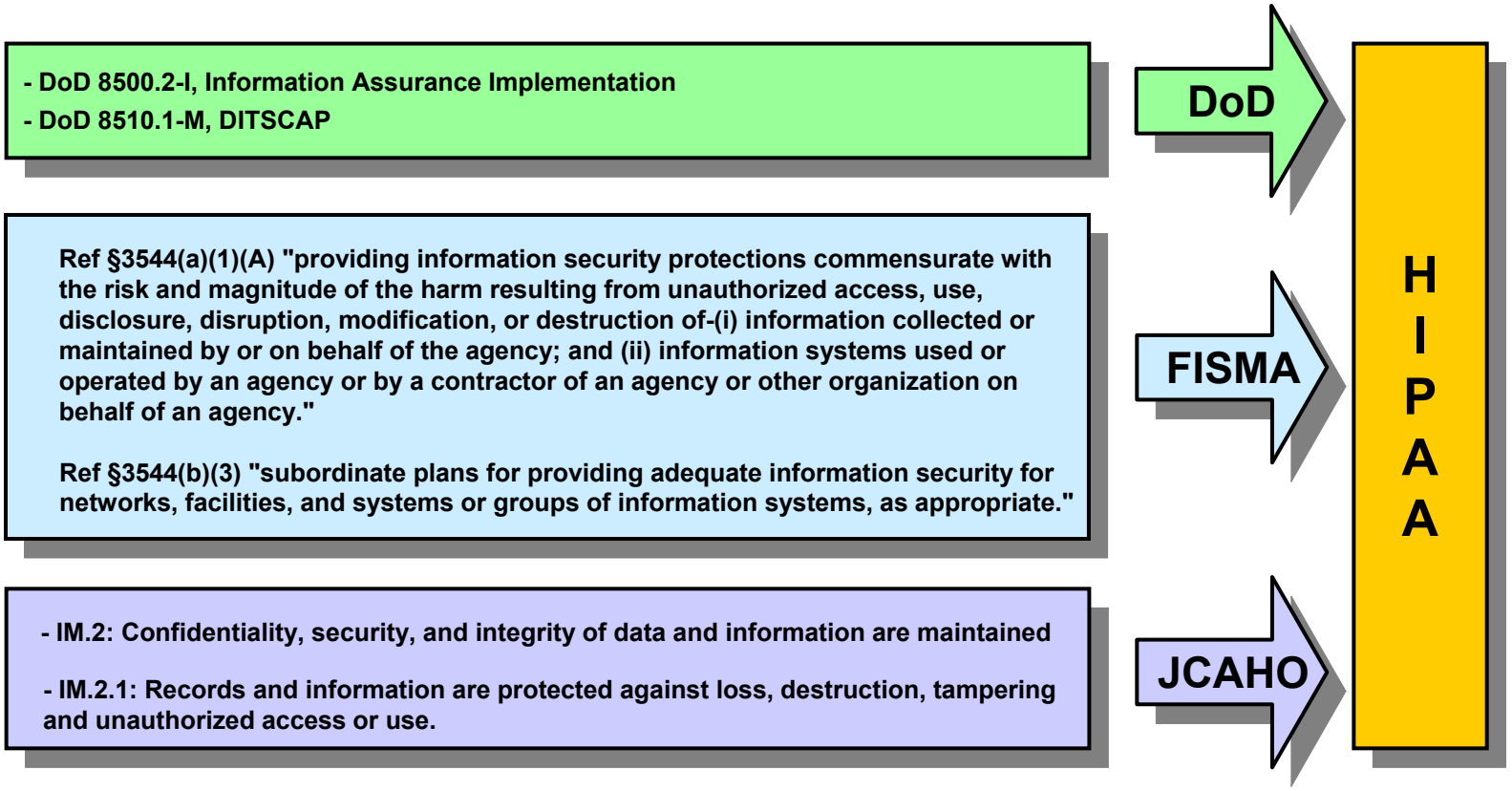
Device and Media Controls (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator

Implementation: Physical Safeguards

Device and Media Controls (5 of 5)

- Sources



Implementation: Physical Safeguards

Activity

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Implementation

Technical Safeguards

- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Implementation: Technical Safeguards

Access Controls (1 of 8)

- Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights
- Three Implementation Specifications are partially addressed by DoD regulations
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption

Implementation: Technical Safeguards

Access Controls (2 of 8)

- **Remember to** establish policies and procedures that enforce administrative access policies
- Establish a formal policy for access control that will guide the development of procedures
- Identify all information systems containing EPHI that are available to authorized personnel
- Determine the scope and degree of access control needed

Access Controls (3 of 8)

- Ensure that system activity can be traced to a specific user
- Ensure that the necessary data is available in the system logs to support audit and other related business functions
- Specify requirements for access control that are both feasible, cost-effective for implementation, and support the business process
- Implement the policy and procedures using a cost-effective hardware/software solution

Access Controls (4 of 8)

- Enforce policy and procedures as a matter of ongoing operations
- Establish procedures for updating access when users require the following:
  - Initial access
  - Increased/decreased access
  - Access to additional information systems
  - Termination of access

Access Controls (5 of 8)

- Ensure only those with a need to know have access to protected data and information systems
- Ensure appropriate segregation of duties when assigning access controls
- **In addition**, identify a method of supporting continuity of operations when the normal access procedures are disabled or unavailable due to system problems or unavailability of key personnel

Implementation: Technical Safeguards

Access Controls (6 of 8)

- **In addition**, based on the organization's risk assessment, implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
- **In addition**, based on the organization's risk assessment, implement a mechanism to encrypt and decrypt EPHI at rest and during transmission

Implementation: Technical Safeguards

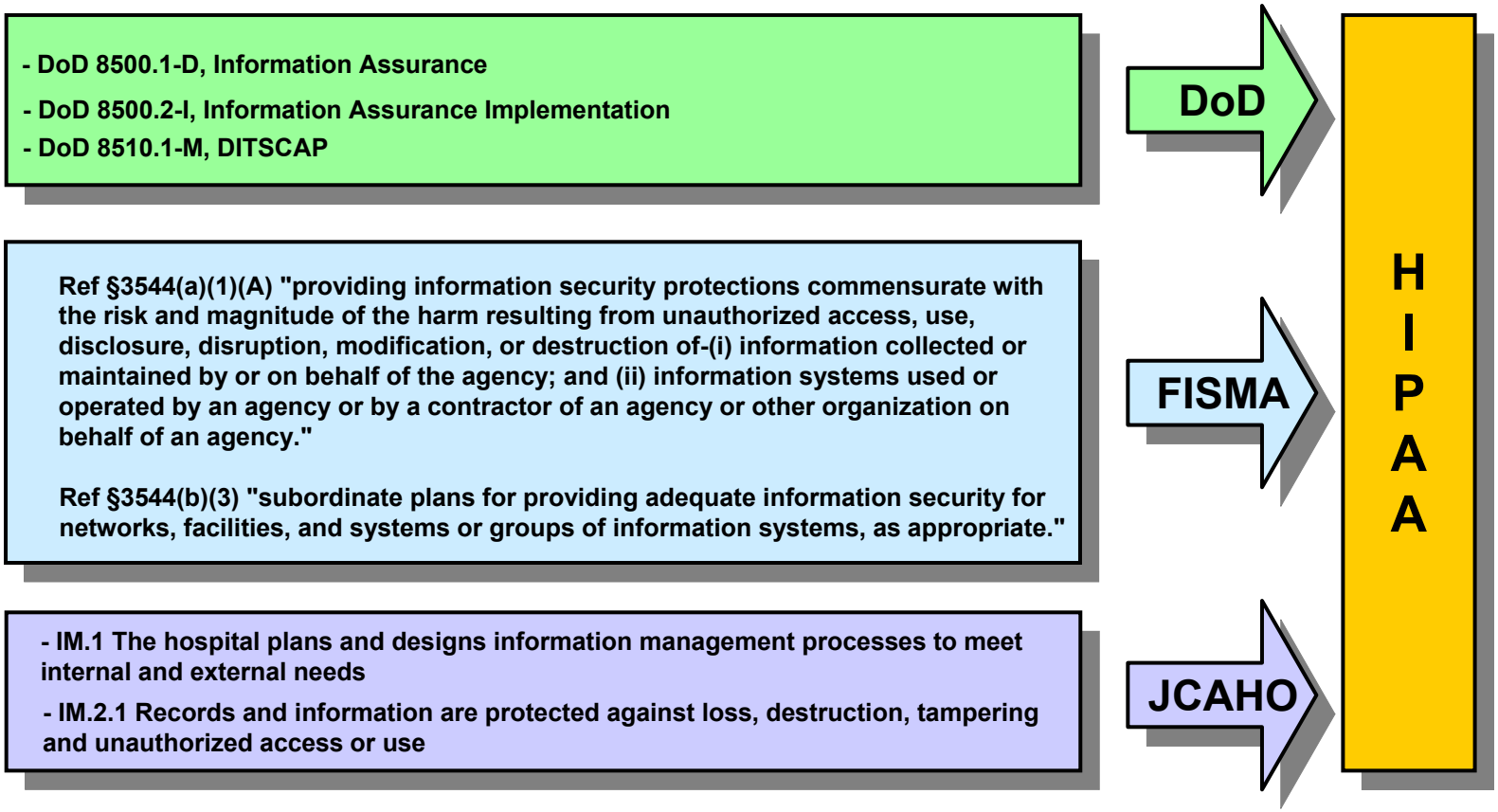
Access Controls (7 of 8)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Technical Safeguards

Access Controls (8 of 8)

- Sources



Implementation: Technical Safeguards

Audit Controls (1 of 5)

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI
- Fully addressed by DoD regulations

Audit Controls (2 of 5)

- **Remember to** determine the appropriate scope of any system audit that will be necessary based on the size and needs of the covered entity
- Use regulatory requirements and the results of your risk assessment to determine which information systems and activities should be tracked and audited
- Determine what data needs to be captured
- Evaluate existing system capabilities and determine if any changes or upgrades are necessary

Implementation: Technical Safeguards

Audit Controls (3 of 5)

- Document and communicate to the workforce the facts about the organization's decisions on audits and reviews
- Determine the types of audit trail data and monitoring procedures that will be needed to derive exception reports
- Activate the necessary audit system
- Begin logging and auditing procedures

Implementation: Technical Safeguards

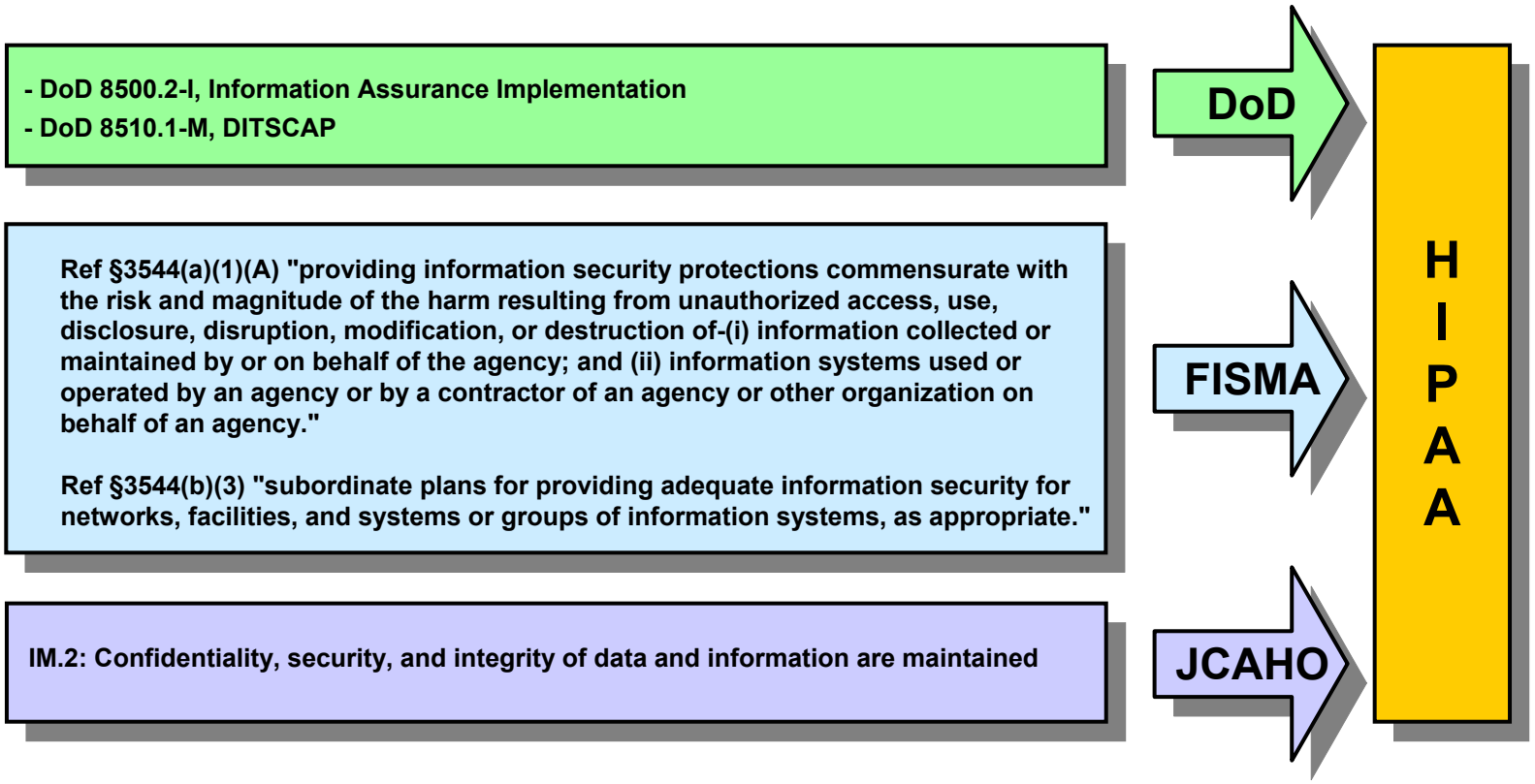
Audit Controls (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Technical Safeguards

Audit Controls (5 of 5)

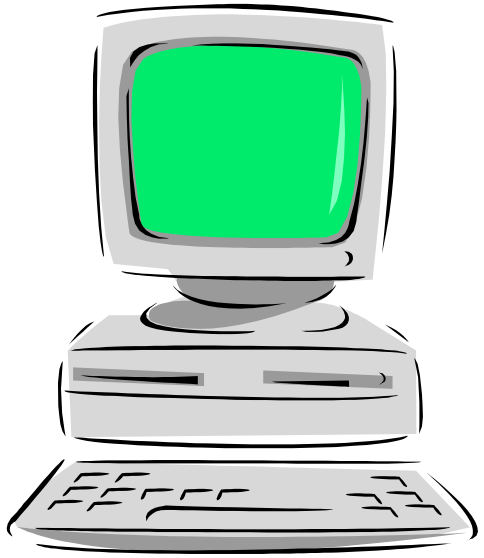
- Sources



Implementation: Technical Safeguards

Integrity (1 of 5)

- Implement policies and procedures to protect EPHI from improper alteration or destruction
- Fully addressed by DoD regulations



Implementation: Technical Safeguards

Integrity (2 of 5)

- **Remember to** identify scenarios that may result in modification to the EPHI (e.g., hackers, disgruntled employees, business competitors, inadequately trained employees)
- Utilize results from risk assessments to identify all authorized users with the ability to create, alter, or destroy data
- Establish a formal (written) set of integrity requirements based on the results of the analysis completed
- Review existing processes to determine if objectives are being met

Implementation: Technical Safeguards

Integrity (3 of 5)

- Identify additional methods if needed to protect the information from modification
- Identify tools and techniques to be developed or procured that support the assurance of integrity
- Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised

Implementation: Technical Safeguards

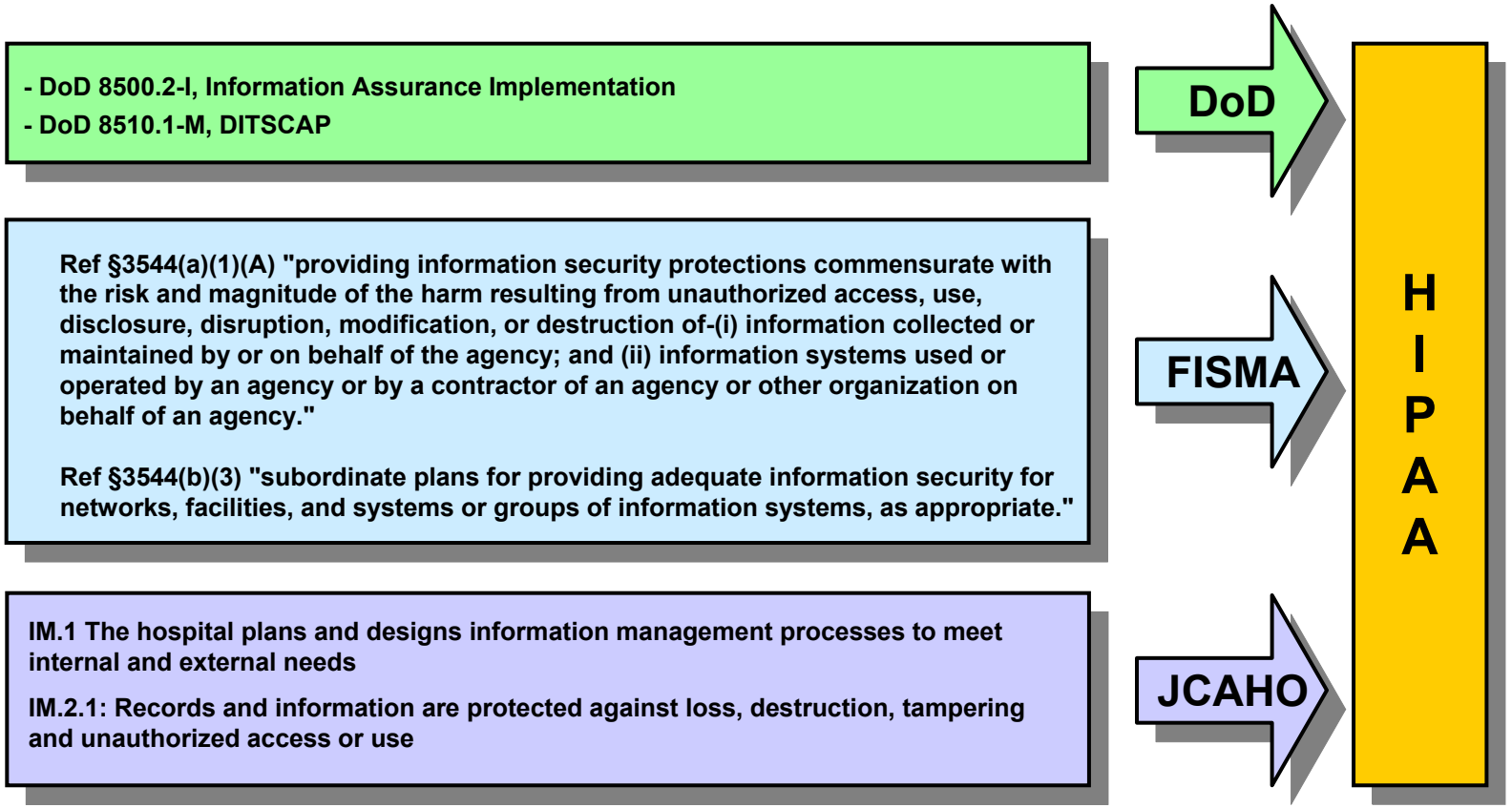
Integrity (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Technical Safeguards

Integrity (5 of 5)

- Sources



Implementation: Technical Safeguards

Person or Entity Authentication (1 of 5)

- Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed
- Fully addressed by DoD regulations

Person or Entity Authentication (2 of 5)

- **Remember to** establish which methods are already in place for authentication
- Determine if additional methods are necessary
- Weigh the relative advantages and disadvantages of commonly used authentication approaches

Person or Entity Authentication (3 of 5)

- There are five commonly used authentication approaches available:
  - Something a person knows, such as a password
  - Something a person has or is in possession of, such as a token (smart card, ATM card, etc.)
  - Some type of biometric identification a person provides, such as a fingerprint, or
  - A combination of two or more of the above approaches
  - Machine to machine (digital certificates)
- Implement the methods selected into your operations and activities

Implementation: Technical Safeguards

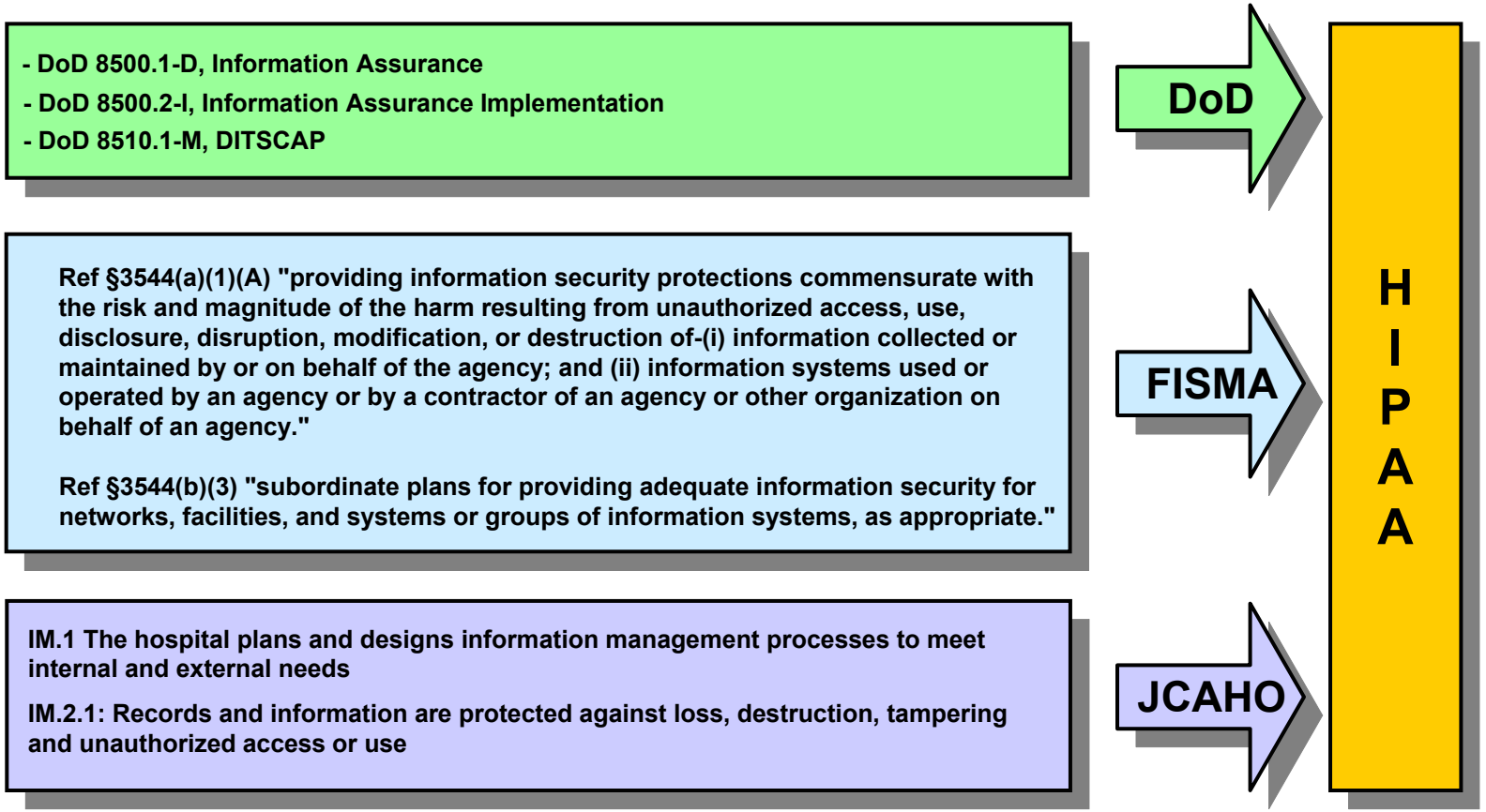
Person or Entity Authentication (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Technical Safeguards

Person or Entity Authentication (5 of 5)

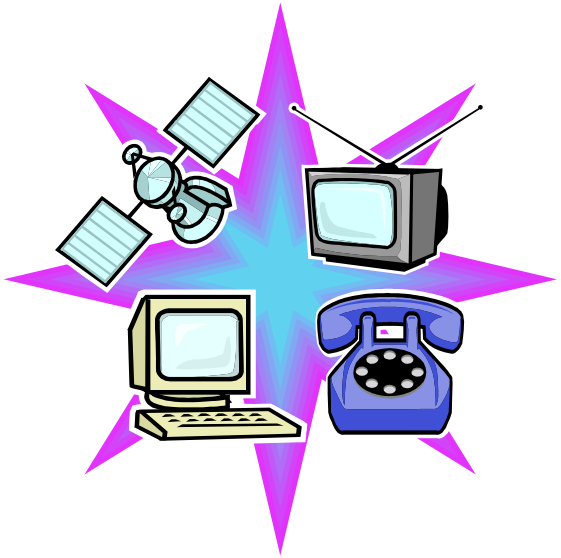
- Sources



Implementation: Technical Safeguards

Transmission Security (1 of 5)

- Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network
- One Implementation Specification is partially addressed by DoD regulations
  - Encryption



Implementation: Technical Safeguards

Transmission Security (2 of 5)

- **Remember to** identify scenarios that may result in disclosure or modification to the EPHI by unauthorized sources during transmission
- Establish a formal (written) set of requirements for transmitting EPHI
- Identify methods of transmission that will be used to protect EPHI
- Identify tools and techniques that will be used to support the transmission security policy

Implementation: Technical Safeguards

Transmission Security (3 of 5)

- **In addition**, based on the organization's risk assessment, implement the encryption of EPHI in transit to protect the confidentiality and integrity of the data during transmission over a network or other electronic means

Implementation: Technical Safeguards

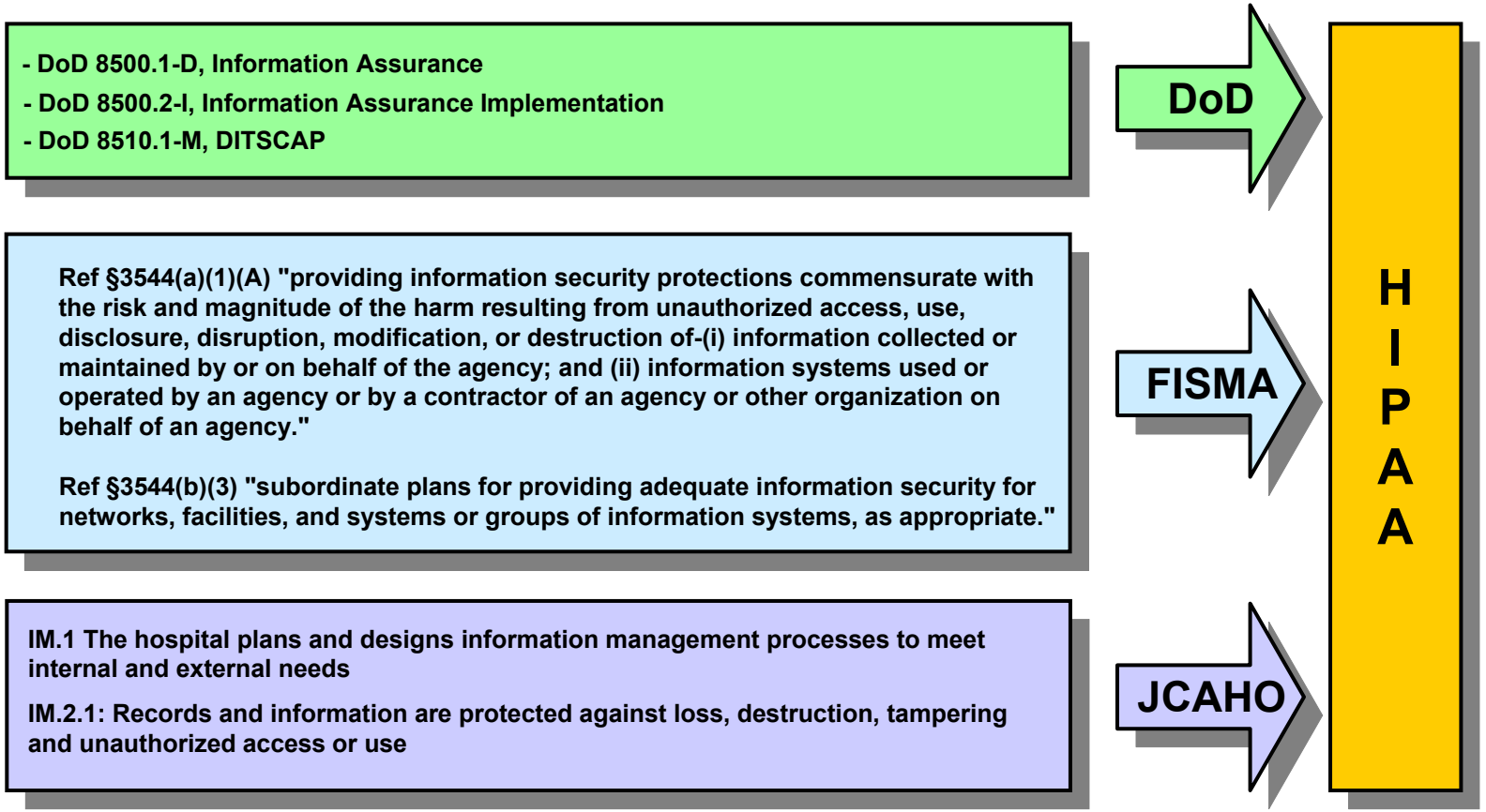
Transmission Security (4 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Implementation: Technical Safeguards

Transmission Security (5 of 5)

- Sources



Activity

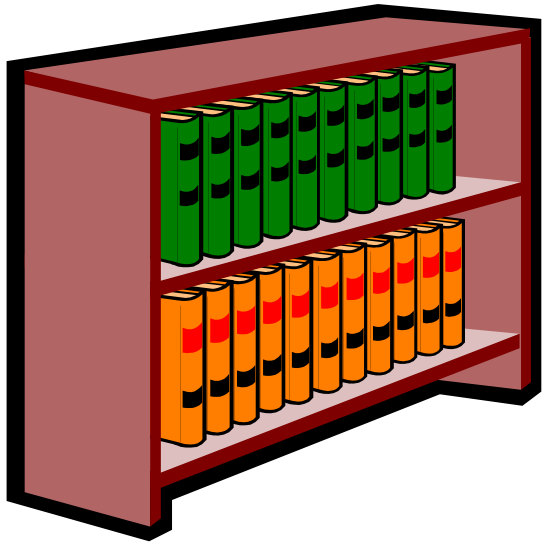
- Review the matrix and add any additional items to the Assessment Phase
- Work within large groups to complete this exercise
- You have 10 minutes

Policies and Procedures and Documentation

- Policies and Procedures
- Documentation

Policies and Procedures (1 of 6)

- Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access to EPHI
- Standard partially addressed by DoD regulations



Policies and Procedures (2 of 6)

- **Remember to** ensure that policies and procedures are developed for:
  - Security Management Process
  - Workforce Security
  - Information Access Management
  - Security Awareness and Training
  - Security Incident Procedures
  - Contingency Plan
  - Business Associate Contracts
  - Facility Access Controls
  - Device and Media Control
  - Access Control
  - Integrity

Policies and Procedures (3 of 6)

- **In addition**, identify methods to ensure the availability of the documentation
- **In addition**, develop a plan to review and update documentation as required

Policies and Procedures (4 of 6)

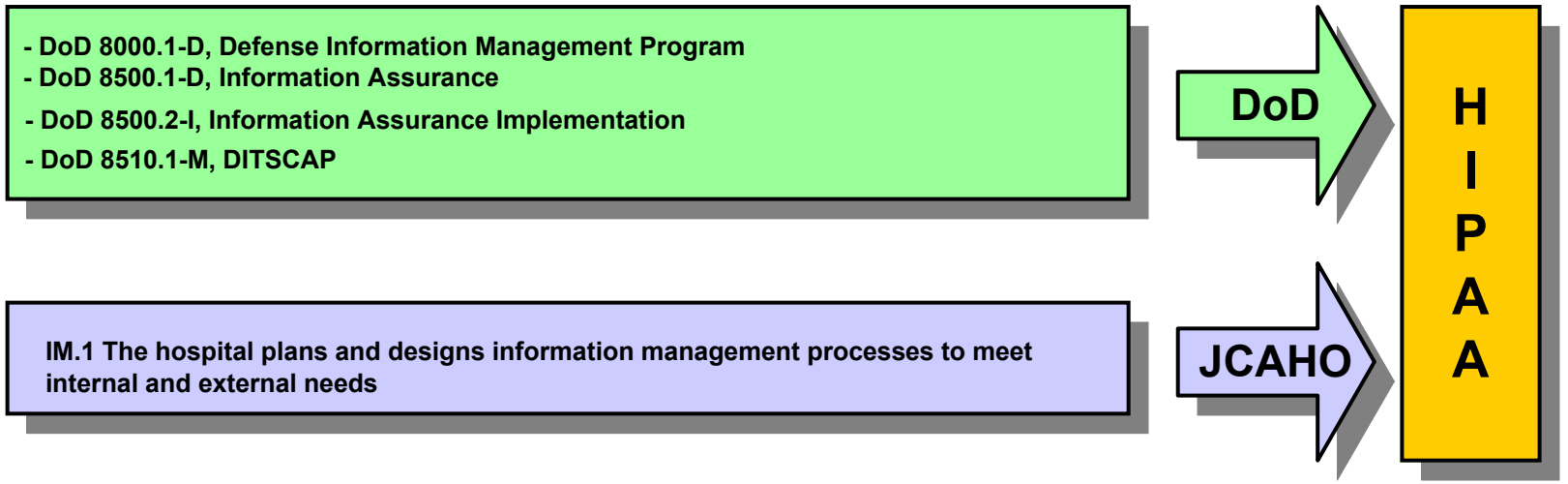
- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

Policies and Procedures (5 of 6)

- Existing activities that support compliance: (Cont.)
  - Physical Security Reviews
    - Physical Security Officer
  - Personnel Reviews
    - Head of Administration Department

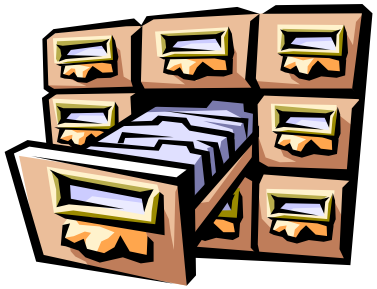
Policies and Procedures (6 of 6)

- Sources



Documentation (1 of 5)

- A covered entity must maintain a written or electronic record of a designation as required by the Security Rule
- Standard and two Implementation Specifications are partially addressed by DoD regulations
  - Availability
  - Updates
- One Implementation Specification is not addressed by DoD regulations
  - Time Limit



Documentation (2 of 5)

- **Remember to** ensure that documentation is provided to those individuals responsible for implementing procedures
- **Remember to** ensure that documentation is reviewed and updated periodically
- **In addition**, develop a plan to ensure that documentation is maintained for 6 years

Documentation (3 of 5)

- Existing activities that support compliance:
  - Certification & Accreditation (DITSCAP)
    - Information Systems Security Manager
    - Information Systems Security Officer
  - FISMA Reviews
    - FISMA Coordinator
  - JCAHO Reviews
    - JCAHO Coordinator
  - IG Inspections
    - Chief Information Officer

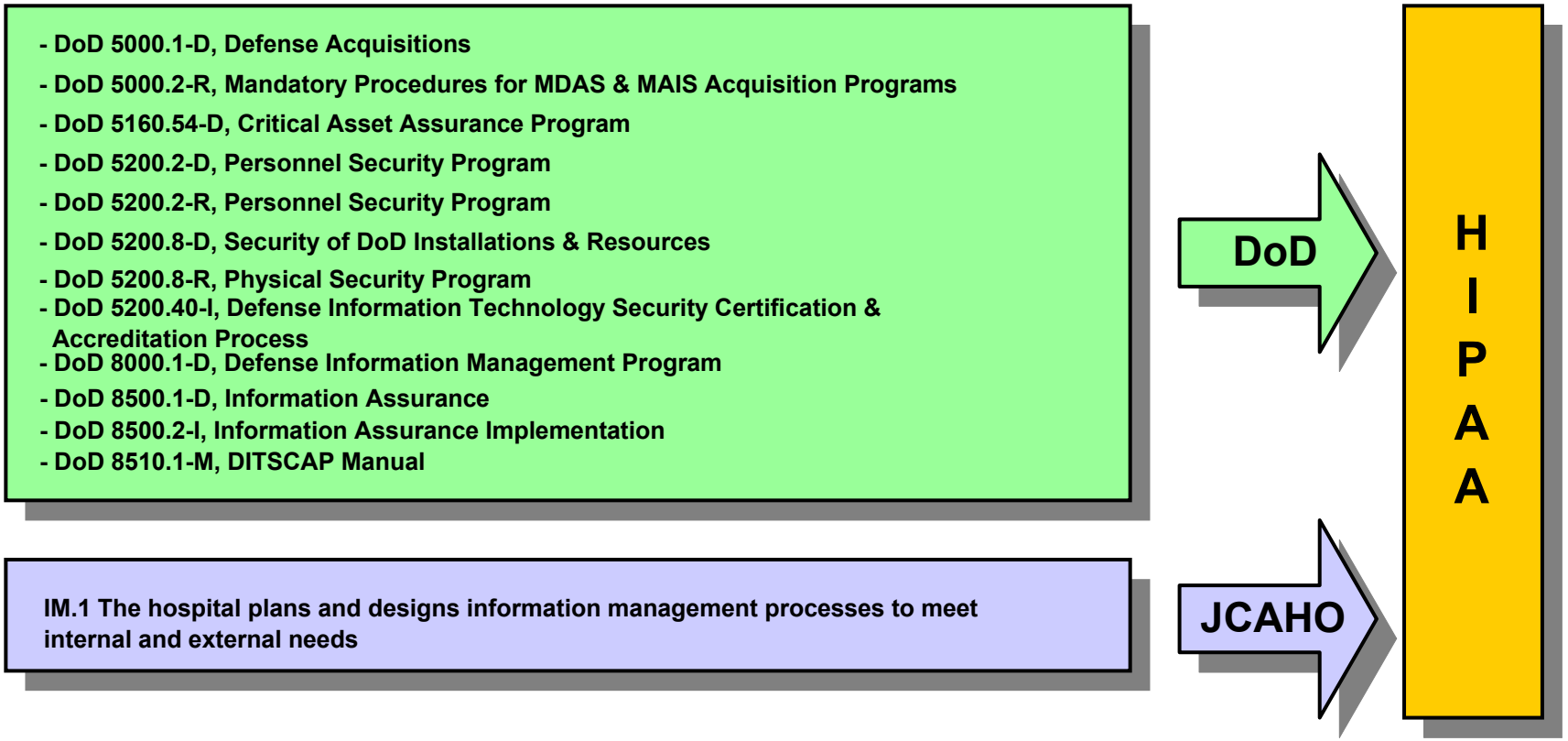
Documentation (4 of 5)

- Existing activities that support compliance: (Cont.)
  - Physical Security Reviews
    - Physical Security Officer
  - Personnel Reviews
    - Head of Administration Department

Implementation: Policies and Procedures and Documentation

Documentation (5 of 5)

- Sources



Summary

- You should now be able to:
  - Identify required steps to comply with each HIPAA security standard
  - Identify current activities that support compliance
  - Identify personnel within your facility that will assist in reaching compliance

Post Compliance Assessment

Activity

- Review the matrix and add any additional items to the Post Assessment Phase
- Work within large groups to complete this exercise
- You have 10 minutes

Presentation Summary

- You should now be able to:
  - Identify the steps required to reach HIPAA security compliance
  - Identify current activities and personnel that will assist you in meeting HIPAA security compliance

Resources

- http://www.tricare.osd.mil/tmaprivacy/HIPAA.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA representatives

HEALTH AFFAIRS

TRICARE
Management
Activity

Please fill out your critique

Thanks!